HISPOL 006.0

The United States House of Representatives Wireless Network Security Policy

CATEGORY: Telecommunications Security

ISSUE DATE: March 27, 2003

The United States House of Representatives
Committee on House Administration

Title:	The United States House of Representatives Wireless Network Security Policy
Number:	HISPOL – 006.0
Category:	Telecommunications Security
Date:	March 27, 2003
Status:	Approved – Committee on House Administration
Purpose:	The purpose of the United States House of Representatives (House) Wireless Network Security Policy is to provide the House user community with a policy governing wireless connectivity to House resources. **THIS POLICY DOES NOT SUPERSEDE REQUIREMENTS OF HOUSE RULES, WHICH GOVERN THE ACTS OF ALL EMPLOYING AUTHORITIES OF THE HOUSE.**
Audience:	This document has relevance to all United States House of Representatives Members, Leadership Offices, Committees, and House staff.
References:	HISPUB 012.0, The United States House of Representatives Wireless Network Security Best Practices Guide HISPOL 002.0, The United States House of Representatives General Information Security Guidelines for Protecting Systems from Unauthorized Use HISPOL 002.1, The United States House of Representatives General Information Security Guidelines to Protect Member and Committee Office Systems from Unauthorized Use

Table of Contents

1.0 INTRODUCTION

The purpose of this policy is to provide guidance for the secure operation and implementation of wireless local area networks (WLANs) and Internet-enabled handheld devices throughout the United States House of Representatives (House) environment. Ensuring sufficient security is a vital concern when designing, deploying, and managing wireless networks and devices. When introducing wireless technologies into the House environment, special care and consideration must be exercised since they introduce both comparable vulnerabilities as in the wired world as well as unique vulnerabilities due to their electromagnetic and portable characteristics.

This policy provides consistent and up-to-date guidance for implementing secure WLANs and Internet-enabled handheld devices in the House environment, and establishes an overarching wireless network security policy that sets the foundation and direction for sound implementation and usage of WLANs and their devices. Since wireless technologies are continuously evolving, it is essential to remain abreast of the current and emerging trends in the technologies and in the security or vulnerabilities of these technologies. This policy is intended to achieve the confidentiality, integrity, availability, and accountability requirements of the House Enterprise data network (wired network) and addresses the minimum requirements for mitigating the risks associated with wireless network device deployment.

1.1 SCOPE

The purpose of this document is to provide the House with guidance for implementing secure wireless networks and the use of Internet-enabled handheld devices (e.g., Personal Digital Assistant [PDA], Tablet PC, or Smart Phone), whether standalone or connected as an extension of the House Enterprise data network. All offices that connect to the House Enterprise data network must follow this policy guidance since the improper introduction of WLANs in one office can create a backdoor and make not only their data and resources vulnerable, but potentially put the entire House Enterprise data network at risk. This policy provides direction to secure transmissions between the wireless station and an access point (AP). A wireless station, or client, is typically a laptop, notebook personal computer (PC), or personal digital assistant with a wireless network interface card [NIC]. The wireless NIC uses radio waves to connect to the WLAN. The access point, which acts as a bridge between the wireless and wired networks, is typically a wired network interface and bridging software. The access point functions as a base station for the wireless network, aggregating multiple wireless stations onto the wired network. This policy serves as the foundation for a comprehensive risk mitigation strategy that is enhanced by published security standards, best practices, policies, and technologies of the wired local area network (LAN).

2.0 POLICY GUIDELINES

It is essential that the following policy guidelines for wireless connectivity to the House data network be observed to ensure the security and integrity of the House-wide systems. All wireless network devices and technologies that provide a bridge between the House Enterprise data network and the wireless network, or any device that is designed to communicate with such a device via the wireless network that do not comply with this policy shall not be permitted to operate. All requests and accompanying justifications for wireless connectivity shall be thoroughly reviewed and approved by the House Information Resources (HIR) Information Systems Security Office (ISSO) before deployment. Only wireless devices and House-owned access points that have been authorized by the HIR ISSO will be permitted to operate and connect to the House Enterprise data network. As part of the overall defense-in-depth strategy of the HIR ISSO, both the wired and wireless networks will be monitored for unauthorized use or devices. WLANs and wireless devices existing throughout the House environment, or connected to the House Enterprise data network, before the establishment of this policy will be audited by the HIR ISSO and required to meet the standards set forth in this policy to continue operating.

Policy guidelines are italicized and in bold; following the policy guidelines are brief explanations that further describe the policy statement specific to the type of wireless solution described.

2.1 AUTHENTICATION

This security service verifies the identity of communicating client stations and provides access control to the network by denying access to client stations that cannot authenticate properly.

All wireless stations (users/devices) must be authenticated to access a WLAN.

- Strong, two-factor authentication (i.e., SecurID, Smart Cards) is recommended.

- If username and password authentication is used, users/devices must use strong passwords (alphanumeric and special character string at least eight characters in length).

All wireless stations (users/devices) must logon to the House Enterprise data network as a separate step from the WLAN authentication procedure before obtaining access to the network.

- Shared secret (or shared key) authentication must be used to authenticate to the WLAN (Shared key authentication uses a “challenge-response” scheme that forces the access point to send a challenge text packet to the wireless station and the station in turn will encrypt the challenge text with its WEP key and send it back to the access

point. The access point will then decrypt the challenge and compare it to the original text sent and if they match, the client is allowed to associate with the access point.) Factory default settings must be changed and unique keys used.

- If a central authentication server or VPN gateway is used in the WLAN architecture, each wireless client must uniquely and successfully authenticate to the WLAN. Strong passwords must be used in this situation.

All wireless device users must be authenticated to access wireless devices and/or the desktop PC synchronization software.

- Wireless handheld devices and synchronization software must require a strong password, a token, or both to authenticate access to the device or software. Users are required to authenticate when operating locally and remotely. If voice authentication is used, password authentication must also be utilized.

- If available, unique device identifiers should be used to authenticate the user for network access to a handheld device.

- The "Power On" password must be enabled on handheld devices.

- Wireless device authentication must not be disabled.

- Timeout mechanisms that automatically prompt the user for a PIN code or password after a period of inactivity must be employed.

2.2 ENCRYPTION

All WLAN traffic must be encrypted to limit eavesdropping and ensure confidentiality.

- Wired Equivalent Privacy (WEP) must be enabled using 128-bit key or the strongest encryption available in the 802.11b compliant product used. Wireless equipment that does not support 128-bit key or greater encryption shall not be used.

- WEP keys must be changed on a frequent, predetermined basis, after a known or suspected compromise, or when there are personnel changes. Avoid changing the WEP key in a predictable manner. If available, fast-key switching shall be used.

- Factory default WEP keys must be changed before deployment. Distinct WEP keys provide more security than default keys and reduce the risk of key compromise. .

- The initialization vector (IV) must be configured to change on a per-transmission basis and in an unpredictable manner (vendor specific).

The WLAN system should make use of at least one of the following capabilities since basic WEP security only is insufficient.

- A solution that meets the proposed 802.1x standard such that it incorporates the Extensible Authentication Protocol (EAP) and an authentication server, whereby users are uniquely authenticated, and dynamic encryption keys are generated per user, per session.

- A virtual private network (VPN) solution shall be used on top of the WLAN as a means of encrypting and authenticating the wireless traffic. It is recommended that either a Layer 2 or a Layer 3 solution be considered.

All wireless handheld devices must encrypt information leaving the device for an adequate level of protection.

- Wireless device default settings must not be set to "no encryption."

- Sensitive data and application data files stored on handheld devices must be protected with robust encryption and password protection utilities. It is required that sensitive data files be deleted from the handheld device once they are no longer needed and archived on a desktop PC.

- A virtual private network (VPN) solution should be used as a means of encrypting and authenticating the wireless traffic. If possible, all wireless communication should use strong cryptography, have robust key management, and have strong user authentication.

- Data residing on external storage modules should be encrypted and stored in a secure manner.

2.3 ACCESS CONTROL

All access to the WLAN system, including its data and resources, shall be restricted unless authorized by the HIR ISSO.

Data traversing wireless networks and data accessible via wireless entry must be protected from unauthorized access, use, modification, or deletion using access control methods.

- To mitigate data leakage, Infrared (IR) ports must be disabled during periods of inactivity.

- File sharing on wireless client devices shall be disabled.

Non-House employees, excluding approved vendors and contractors, must not have access to WLANs that connect to the House Enterprise data network.

- Service Set IDs (SSIDs) must be changed from the factory default to something that is meaningless to outsiders. SSID character strings must not reflect Member or Committee name, location, or product being used.

- Broadcast mode of SSIDs must be disabled in products that permit it so that the client SSID must match that of the access point.

- Where possible, the wireless network should be configured with the longest beacon interval.

- If employing a WLAN solution that utilizes WEP as defined in the 802.11b standard, then Media Access Control (MAC) address filtering shall be used if the product permits it.

- The authentication server, firewall, and/or VPN gateway must enforce access control mechanisms.

2.4 ANTIVIRUS SOFTWARE

All WLANs and handheld devices must utilize antivirus software as directed in HIR Security Policy.

- Antivirus software for handheld devices shall scan all entry ports (i.e., beaming, synchronizing, email, and Internet downloading) as data is imported into the device, provide online signature update capabilities, and prompt the user before it deletes any suspicious files.

2.5 PERSONAL FIREWALLS

Personal firewall software helps mitigate threats of confidentiality, integrity, and authenticity of information being transferred over the Internet.

It is highly recommended that WLAN client and handheld devices utilize personal firewall software.

- Users that access public wireless networks (e.g., in airports, conference centers, coffee shops) should install personal firewall software on all WLAN client and handheld devices. A personal firewall protects against wireless network attacks and rogue access points (e.g., Ad hoc networks, accidental or malicious association, soft access points) that can be easily installed in public areas.

2.6 PHYSICAL SECURITY

The physical security of all wireless access points and handheld devices is the first line of defense in WLAN security. It is essential that proper physical countermeasures be in place to mitigate risks such as theft of equipment, insertion of rogue access points, and wireless network monitoring devices.

Access points must be physically secured upon proper configuration to prevent tampering and reprogramming (i.e., to prevent unauthorized physical access).

- Access points must be placed in secure areas, such as high on a wall, in a wiring closet, or in a locked enclosure to prevent unauthorized physical access and user manipulation. Devices must not be placed in easily accessible public locations.

- To mitigate eavesdropping, access points shall be placed strategically within the building so that the range does not exceed the physical perimeter of House-controlled facilities and allow unauthorized users to eavesdrop near the perimeter. Access points shall be placed to minimize or prevent the distance that the signal can travel outside the area that is under the control of the organization, including buildings, court yards, adjacent parking areas, etc.

- In areas where utilization is not required on a 24 hours per day, 7 days per week basis, access points shall be turned off during all hours during which they are not used (e.g., after hours and on weekends) to minimize potential exposure to malicious activity.

- The transmission power of WLAN access points must be restricted to the lowest power required for coverage.

- In the event that the reset function of an access point is used, the device must be restored to the latest security settings.

Wireless handheld devices and Network Interface Cards (NICs) must be physically protected from loss and theft.

- Wireless handheld devices, backup modules, and NICs (e.g., laptop computers) must be stored in a secure area, such as a desk with drawers that lock, or a file cabinet that locks when they are not being used.

- It is recommended that software that automatically deletes all data after a preset number of failed login attempts be installed on handheld devices.

2.7 LOGICAL SECURITY

All wireless LAN access points and handheld devices must be authorized.

All access points shall be logically separated and isolated from the House Enterprise data network, such as on a different segment, in a demilitarized zone (DMZ), or in a virtual LAN (VLAN).

- WLANs must be treated as insecure counterparts to their wired associates. Access to resources on the wired network must be restricted.

All access points must be firewall protected outside the wired network.

Placement of access points and channel assignments shall be such that coverage/throughput is maximized while interference (denial of service) is kept to a minimum between different access points or WLANs.

- Access points shall be physically situated so that authorized users can connect, yet away from sources of interference such as microwave ovens and Bluetooth devices.

- To keep interference to a minimum, access point channels shall be at least five channels different from all other nearby access points on different WLANs. Some coordination may be required if multiple WLANs are to be used within close proximity.

All insecure and nonessential management protocols (Hypertext Transport Protocol (HTTP) and Simple Network Management Protocol (SNMP)) shall be disabled.

- If SNMP is turned on for management purposes, the SNMP Community Strings must be changed from their manufacturer default to unique and difficult to guess strings.

- SNMP settings must be set to least privilege (read only).

- Web-based management of access points shall be from pre-defined management stations controlled by access lists on the access point. SNMP requests shall only be accepted from specified management devices.

- SNMPv3 products or equivalent cryptographically protected protocol shall be used since they include mechanisms to provide strong security.

2.8 INVENTORY, MONITORING AND AUDIT

All wireless access points must meet the current security configurations established by the HIR ISSO.

All wireless LANs and handheld devices must be routinely monitored and security audits performed to verify that security configurations comply with this policy, access points and wireless devices are authorized, and to identify unauthorized activity.

- The ISSO will conduct yearly audits of access points to ensure that security configurations conform to this policy and HISPUB 012.0 (The United States House of Representatives Wireless Network Security Best Practices Guide), and to maintain a current inventory of the devices.

- If DHCP is used in the environment, logs shall be reviewed for static addresses to determine if rogue access points have been installed.

- Access logs and system audit trails shall be routinely monitored.

- The ISSO will conduct routine controlled penetration tests or packet sniffing/wireless traffic analysis on WLANs and within the coverage area.

- All access points must have Intrusion Detection Systems (IDS) at designated areas on House property to detect unauthorized access or attack.

Procedures must be established and followed for the inventory and control of wireless devices and equipment.

2.9 SYSTEM ADMINISTRATION / VENDOR RESPONSIBILITIES

It is the System Administrator's / Vendor's responsibility to ensure that Wireless LANs and devices meet the technical standards outlined in this policy at all times.

System Administrators / Vendors are required to operate Wireless LANs and devices in a secure manner.

- This includes, but is not limited to, proper authorization and termination of access, proper configuration and placement of wireless components and associated security technologies, routine, random, and event-driven maintenance, support monitoring and audit functions, etc.

- System Administrators / Vendors are required to change factory default settings and use strong administrative passwords on all wireless devices to ensure a higher level of security. (On some wireless devices, the factor default password is blank.) All insecure and nonessential management protocols must be disabled.

- To the extent possible, System Administrators / Vendors shall ensure that their wireless implementation and associated security technologies are up-to-date with evolving standards and best practices. Client NICs, access points, and handheld

devices must support firmware upgrade so that security patches and upgrades may be fully tested and deployed as they become available.

- System Administrators / Vendors are required to maintain a list of authorized wireless device users to enable them to perform periodic inventory checks and security audits.

2.10 USER RESPONSIBILITIES

It is the wireless user's responsibility to comply with this policy.

Wireless users must only access information systems using approved wireless device hardware, software, solutions, and connections.

- Wireless device hardware, software, solutions, and connections that do not meet the standards of this Policy shall not be authorized for deployment.

Wireless users must act appropriately to protect information, network access, passwords, cryptographic keys, and wireless equipment.

Wireless users are required to report any misuse, loss, or theft of wireless devices or systems immediately to the HIR Information Systems Security Office at (202) 226-4988.